

Claims

What Is Claimed Is:

- 5 1. A method for providing non-repudiation of transaction information that includes mark up language data, comprising:
 - (a) receiving a confirmation request form from a server for digital signing by a digital signing process;
 - 10 (b) temporarily maintaining the confirmation request form in volatile memory associated with a client unit;
 - (c) presenting a copy of the temporarily maintained confirmation request form for display to a user; and
 - (d) digitally signing the temporarily maintained confirmation request form in response to confirmation data received in response to displaying the copy of the temporarily maintained original transaction data.
- 15 2. The method of claim 1 wherein the confirmation request form includes at least one mark up language form that includes user entered data, at least one field name and form formatting information, all of which are presented for display to the user for acceptance and for receiving a digital signature.
- 20 3. The method of claim 1 including the step of:
 - 25 (e) sending the signed confirmation request form to a server for signature verification wherein the server compares a stored copy of the confirmation request form as it existed prior to receiving the digital signature, with the received digitally signed confirmation request form.

4. The method of claim 1 wherein the received confirmation request form is sent by a server that also provides incomplete mark up language form data from which the received confirmation request form was based.

5

5. The method of claim 1 wherein the step of receiving the confirmation request form includes receiving a transaction confirmation request from a server.

10

6. The method of claim 1 wherein steps (a) and (b) are performed under control of a non-proxy cryptographic software application.

7. The method of claim 6 wherein step (c) is performed under control of a web browser.

8. A method for providing non-repudiation of transaction information that includes mark up language data, comprising:

(a) receiving, by a web browser associated with a client unit, an incomplete mark up language form, including at least one field name and form formatting information, for use in completing an electronic transaction with a receiving unit;

(b) presenting, by the web browser, the incomplete mark up language form for completion and submission to the receiving unit;

(c) launching, in response to a completed form submission request, a non-proxy cryptographic application and sending through the non-proxy cryptographic application, at least user entered data and an associated field name for the receiving unit;

(d) receiving back from the receiving unit, a transaction confirmation request including a confirmation request form that includes the at least user entered data, the associated field name and the form formatting information, for digital signing by the non-proxy cryptographic application;

(e) temporarily maintaining, under control of the non-proxy cryptographic application, the confirmation request form in volatile memory associated with the client unit;

(f) presenting a copy of the temporarily maintained confirmation request form, by the web browser, for display to a user; and

(g) digitally signing, by the non-proxy cryptographic application, the temporarily maintained confirmation request form in response to confirmation data entered by the user in response to displaying the copy of the temporarily maintained original transaction data.

9. The method of claim 8 including the step of:

(h) sending the signed confirmation request form to the receiving unit for signature verification wherein the receiving unit

compares a stored copy of the confirmation request form as it existed prior to receiving the digital signature, with received digitally signed confirmation request form.

- 5 10. The method of claim 9 wherein the non-proxy cryptographic application is an applet.
11. The method of claim 9 including the step of digitally signing, by the receiving unit, the received digitally signed confirmation request form if the comparison
- 10 indicates that it matches the stored copy of the confirmation request form.

12. An apparatus for providing non-repudiation of transaction information that includes mark up language data, comprising:
- at least one processing unit;
 - volatile memory, operatively coupled to the processing unit,
 - 5 non-volatile memory, operatively coupled to the processing unit, containing a web browser and a non-proxy cryptographic application wherein the non-proxy cryptographic application receives confirmation request form from a server for digital signing by the non-proxy cryptographic application, temporarily maintains the confirmation request form in the volatile memory, and wherein the web browser presents a copy of the temporarily maintained confirmation request form for display to a user [to prevent tampering]; and wherein the non-proxy cryptographic application digitally signs the temporarily maintained confirmation request form in response to confirmation data received in response to displaying the copy of the temporarily maintained original transaction data.
- 10
13. The apparatus of claim 12 wherein the confirmation request form includes at least one mark up language form that includes user entered data, at least one field name and form formatting information, all of which are presented for display to the user, by the web browser for acceptance and to the non-proxy cryptographic application to receive a digital signature.
- 15
14. The apparatus of claim 12 wherein the non-proxy cryptographic application sends the signed confirmation request form to the server for signature verification.
- 20
15. The apparatus of claim 12 wherein the received confirmation request form is sent by a server that also provides the non-proxy cryptographic application with initial unpopulated transaction mark up language form data from which the received confirmation request form was based.
- 25
- 30

16. The apparatus of claim 12 wherein the non-proxy cryptographic application receives a transaction confirmation request from a server.

5

17. A storage medium comprising:

memory containing executable instructions that when read by one or more processing units, causes the one or more processing units to:

5 receive confirmation request form from a server for digital signing
by a digital signing process;
temporarily maintain the confirmation request form in volatile
memory associated with a client unit;
present a copy of the temporarily maintained confirmation request
form for display to a user; and
10 digitally sign the temporarily maintained confirmation request
form in response to confirmation data received in response to displaying
the copy of the temporarily maintained original transaction data.

18. The storage medium of claim 17 wherein the confirmation request form includes at
15 least one mark up language form that includes user entered data, at least one field
name and form formatting information, all of which are presented for display to the
user for acceptance and for receiving a digital signature.

19. The storage medium of claim 17 wherein the memory includes executable
20 instructions that when executed by the one or more processing units causes the one or
more processing units to send the signed confirmation request form to a server for
signature verification.

20. The storage medium of claim 17 wherein the step of receiving confirmation request
25 form includes receiving a transaction confirmation request from a server.